

GS Advanced Program 2023

Generic Booklet

Test Name/Code/No. : 693031

Name			
Email ID.			
Roll No.			
Mobile No.		Date	

Allotted Time : 60 Minutes

Instructions to Candidates -

- There are 7 Questions in this Question paper.
- All Questions are Compulsory.
- For all updates, please visit the noticeboard - <https://noticeboard.forumias.com/gsap-2023/>

Important -

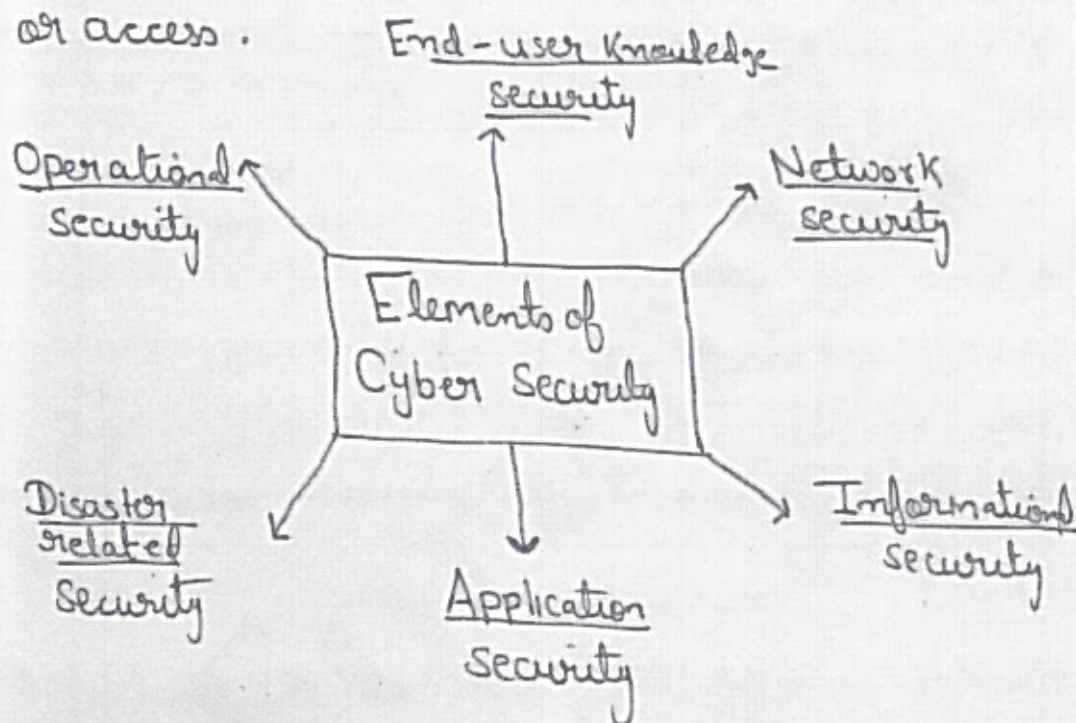
- Answers must be attempted in the QCA Booklet only.
- To upload the Answer Copies please visit to "My Course" section on - <https://academy.forumias.com/>
- Only those copies will be evaluated which will be submitted before the next class.

Q. No.	Grade/Score
1	
2	
3	
4	
5	
6	
7	
Overall Grade/Score	

Start Writing Here

(1)

Cyber security refers to techniques of protecting computer networks, programs and data from unauthorised attacks or access.



Challenges to cyber security :

Technical

→ IT Revolution has provided easy access to technology ⇒ entities with malicious intent can very easily threaten cyber security

- Big data is known for its — Volume, Velocity & Variety $\Rightarrow$ very challenging to monitor & protect
- Cyber attacks are covert, hence hard to trace the source

Economic

- Cyber attacks being done for financial gains
- Low cost infra required $\Rightarrow$ Non-State actors can also use [Cyber Terrorism]
Eg ISIS's attack on 2000 Indian websites

Geopolitical

- Adversary countries using cyber space as 5th arena of warfare Eg - STUXNET,
Eg - Recent attack on AIIMS data from China.

Other

- Trans-national crime $\Rightarrow$ Require multilateral effort
 A robust vigilance & response system at national & international level is required to curb the menace & harness 4th I.R.

Overall Grading (✓)

Poor			Average			Good		
1	2	3	4	5	6	7	8	9

- 2) Recently, WEF in its Global Cyber Security Outlook highlighted various emerging challenges & threats in cyberspace in near future.

Need for securing Cyber Space :

- China is scaling up its Cyber warfare & espionage capacity at ~~very~~ unprecedented level [Joint report by CIA & MI-5]
- Data has become the "new oil"
 - ⇒ Protecting it [raw material of cyber space] has become important.
- Emerging technologies like Pegasus work on 'Zero-click' model
 - ⇒ mere cyber hygiene no more important now we need cyber security
- Country's Critical infrastructures can now be at risk through cyber space
 - Ex - STUXNET → Iran's Nuclear facility attacked
 - Ex - Attack on Kudankulam Nuclear Plant [T.N.]

→ Age of 4th IR where governments and corporates around the world are pushing for digital first.

→ Increasing no. of people on internet
Eg - India alone has >800Mn [2022]

→ Cyber terrorism is also on rise.
Eg - ISIS's goal for "Universal Cyber Caliphate"

Government Initiatives

- ① CERT-In : Nodal for cyber crimes
- ② Cyber Swachhata Kendras : Be virus/malware free.
- ③ National Critical Info Infra Protection Centre
- ④ National Cyber Crime Coordination Centre
- ⑤ Kerala's Cyber dome

International Initiatives

- ① Budapest Convention
- ② Paris CALL
- ③ ITU

Thus, coordinated efforts & capacity building at national & international level are need of the hour

Overall Grading (✓)

Poor			Average				Good		
1	2	3	4	5	6	7	8	9	

- 3) After land, water, air & space, now Cyber space has become 5th arena of warfare.

Reasons for Cyber space being named so:

- ① Nations involving in cyber warfare
Eg- STUXNET → attack by USA & Israel on Iran's nuclear facility
- ② Increasing stakes in cyber space/digital space.
Eg - India's Aadhar data
⇒ "Data is the new oil"
- ③ Non-state actors using cyber-space for terrorism & organised crimes
Eg - ISIS's attack on 2000 Indian websites
Eg - Use of Dark web.
- ④ As of now, there is a lawlessness (at global level) in cyber space.

Reasons for countries preferring Cyber war :-

- ①. Anonymous attacks can be made which are hard to trace.
 - ②. No loss of life unlike conventional wars
 - ③. Input cost is very low when compared to conventional wars.
 - ④. No limiting international convention [like some UN agreement]; conventional wars have many — ~~Cy~~ - Vienna Convention
 - ⑤. From Globalisation, world has moved to "Cyberisation" $\Rightarrow$ a lot is at stake in cyber space.
- "The problems of digital space are now spilling into matters of national security & hence require comprehensive efforts" [PM Modi]

Overall Grading (✓)

Poor			Average			Good		
1	2	3	4	5	6	7	8	9

- 4) Cyberspace has become the 5th arena and 4th dimension of warfare in this data-intensive digital world.

India's National Cyber security Policy, 2013
has some of the ^{good} features as:

- Different bodies for different level of threats & a national level nodal agency
- Formation of NCIIPC
- 5,00,000 trained cyber-security personnel
- Promoting PPP model
- Learning from the global best practices
- Setting up test labs for regularly checking the safety of equipments used in the country
- Push for multilateral & bilateral collaboration
- Promote indigenous technology through R & D

However, despite the above positive features, the policy has some drawbacks:

- It talks only about defensive measures & ignores offensive capacity building
- It does not give a road map for its implementation
- Provisions like "digitally armed Force" of 5,00,000 personnel still in curtains
- Cyberspace has changed massively in last decade and hence the policy needs to be updated.

Hon'ble IT Minister Ashwini Vaishnaw recently said in the winter session that the Ministry is working on a new Cyber security Policy. This would be a welcome step

Overall Grading (✓)

Poor			Average			Good		
1	2	3	4	5	6	7	8	9

- 5) Hon'ble PM Narendra Modi recently highlighted that the problems of digital world are no more confined to the cyber space, but have become matters of national security

^{cyber}
Types of threats to which India is vulnerable to:

① Cyber Warfare

- Part of China's 3 dimensional warfare strategy against India
 - ↳ scaling up its offensive cyber warfare capabilities [CIA report]
 - ↳ engaging in covert warfare against India.
- Eg → AIIMS - data of 3.2 Crore people hacked
 - 6000 attempts on ICMR's website in 24 hours [Dec 2022] ; Both by Chinese hackers

② Cyber crimes / attack

- India has 2nd largest Internet users base with >800 mn users [IMAI report, 2022]
- India is 5th most vulnerable country to cyber attacks
- Cyber crimes in India increased by 90% in 2020 [CERT-In]
- Cyber attacks costed \$4Bn ; expected to increase to \$80Bn in 10yrs [WEF]
 - ⇒ Global menace.
- The country is seeing "Digital First" in all arenas.
 - Ex - 70% increase in online economic transactions in last 3 years.

③ Cyber Terrorism

→ Terrorist groups using cyber-space to threaten sovereignty of India

Eg - ISIS's attack on 2000 Indian website

→ Country's Critical infra at risk

Eg - Kudankulam Power Plant cyber attack

Eg - West Bengal State Discom attack (2017)

④ Cyber espionage

→ Increased digital snooping & ransomware

Eg - Pegasus ; Wanna Cry.

Way Forward

- ① Follow 'Zero Trust Model'
- ② Promoting Cyber hygiene & awareness
- ③ Promoting R & D
- ④ Implementing Data Protection Bill, 2022
- ⑤ Making a standalone comprehensive legislation

Overall Grading (✓)

Poor			Average			Good		
1	2	3	4	5	6	7	8	9

Q.6)

Money laundering refers to conversion of money which has been illegally obtained in such a manner that it appears legal.

Increasing significance post 9/11 :

→ USA's Global war on Terrorism [GWOT] choked illegal fundings of terror outfits

↳ So, shifted to Money laundering [ML]

→ Rise in organised crime in last 20 years.

→ 20th century was an era of state actors ; 21st is that of non-state actors — MNCs, NGOs, Terror groups

↳ All have entities that engage in ML

→ Globalisation has made transit of people & money across boundaries very easy

→ IT revolution further supported growth of ML due to sophisticated methods

Source of Funding of terrorist activities

- Nexus/Linkage between Organised Crimes & Terrorist groups
 - ↳ Both using ML for financing the other
- Creation of a Parallel economy
- Easier access — Hawala, Cryptos, NFTs etc.

Way forward by FATF

- Globalize based on Vienna Convention on ML
- Scrutinise NGOs
- International co-operation
- Empower law enforcement agencies

Overall Grading (✓)

Poor			Average			Good		
1	2	3	4	5	6	7	8	9

Cryptocurrencies & NFTs are types of virtual/digital assets with associated monetary value.

Both have emerged as methods to launder money :

→ "Decentralised currencies"

↳ hence used by non-state actors

→ Away from regulatory oversights of state/govt

↳ used to fund illicit activities

- Difficult to trace the source
- Done on digital medium
 - ⇒ Easier movement across the globe
- Gaining prominence in transactions
 - Eg - \$2.8 Bn was laundered in Bitcoins in 2019 [Crypto Anti ML report]
- Easier than conventional laundering methods like Hawala, Round tripping etc.

Way Forward

- International cooperation between nations & bodies like FATF, WCO, BASEL etc.
- Making them legal
 - ↳ will prevent somewhat from being underground

Overall Grading (✓)

Poor	Average			Good		
	4	5	6	7	8	9